Controls against Attacks

Dr. Bhaskar Mondal

Computer Forensics Against Computer Crime

- Technology
- Law Enforcement
- Individual and Societal Rights
- Judiciary
- …

Methods of Defense

- Five basic approaches to defense of computing systems
  - Prevent attack
    - Block attack / Close vulnerability
  - Deter attack
    - Make attack harder (can't make it impossible ☹)
  - Deflect attack
    - Make another target more attractive than this target
  - Detect attack
    - During or after
  - Recover from attack

A) Controls

- Castle in Middle Ages
  - Location with natural obstacles
  - Surrounding moat
  - Drawbridge
  - Heavy walls
    - Arrow slits
    - Crenellations
  - Strong gate
    - Tower
  - Guards / passwords

- Computers Today
  - Encryption
  - Software controls
  - Hardware controls
  - Policies and procedures
  - Physical controls

A) Controls

- Medieval castles
  - location (steep hill, island, etc.)
  - moat / drawbridge / walls / gate / guards /passwords
  - another wall / gate / guards /passwords
  - yet another wall / gate / guards /passwords
  - tower / ladders up

- Multiple controls in computing systems can include:
  - system perimeter – defines „inside/outside”
  - preemption – attacker scared away
  - deterrence – attacker could not overcome defenses
  - faux environment (e.g. honeypot, sandbox) – attack deflected towards a worthless target (but the attacker doesn’t know about it!)
- Note layered defense /
- multilevel defense / defense in depth (ideal!)

Tools for Information Security

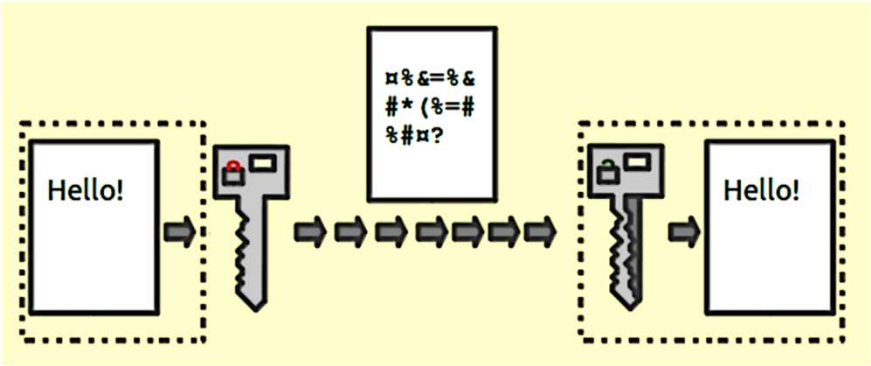
Confidentiality	Integrity	Availability
• Encryption • Password • Two-factor authentication • Biometric verification	• Encryption • User access controls • Version control • Backup and recovery procedures • Error detection software	• Off-site backups • Disaster recovery • Redundancy • Failover • Proper monitoring • Environmental controls • Virtualization • Server clustering • Continuity of operations planning

Controls: Encryption

- Primary controls!
- Cleartext scambled into ciphertext (enciphered text)
- Protects CIA:
  - confidentiality – by “masking” data
  - integrity – by preventing data updates
    - e.g., checksums included
  - availability – by using encryption-based protocols
    - e.g., protocols ensure availablity of resources for different users

Encryption

- An algorithm (program) encodes or scrambles information during transmission or storage
- Decoded/unscrambled by only authorized individuals to read it
- How is this done?
  - Both parties agree on the encryption method (there are many) using keys
    - Symmetric key – sender and receiver have the key which can be risky
    - Public Key – use a public and private key where the public key is used to send an encrypted message and a private key that the receiver uses to decode the message



Controls: Software Controls

- Secondary controls – second only to encryption
- Software/program controls include:
  - OS and network controls
    - E.g. OS: sandbox / virtual machine
    - Logs/firewalls, OS/net virus scans, recorders
  - independent control programs (whole programs)
    - E.g. password checker, virus scanner, IDS (intrusion detection system)
  - internal program controls (part of a program)
    - E.g. read/write controls in DBMS
  - development controls
    - E.g. quality standards followed by developers
      - incl. testing

- Considerations for Software Controls:
  - Impact on user’s interface and workflow
    - E.g. Asking for a password too often?

Controls: Hardware Controls

- Hardware devices to provide higher degree of security
  - Locks and cables (for notebooks)
  - Smart cards, dongles, hadware keys, ...
  - ...

Controls: Policies and Procedures

- Policy vs. Procedure
  - Policy: *What* is/what is not allowed
  - Procedure: *How* you enforce policy

- Advantages of policy/procedure controls:
  - Can replace hardware/software controls
  - Can be least expensive
    - Be careful to consider *all* costs
      - E.g. help desk costs often ignored for for passwords (=> look cheap but migh be expensive)

Policy - must consider

- Alignment with users' legal and ethical standards
- Probability of use (e.g. due to inconvenience)

  Inconvenient: 200-character password,
  change password every week

  (Can be) good: biometrics replacing passwords
- Periodic reviews
  - As people and systems, as well as their goals, change

Controls: Physical Controls

- Walls, locks
- Guards, security cameras
- Backup copies and archives
- Cables an locks (e.g., for notebooks)
- Natural and man-made disaster protection
  - Fire, flood, and earthquake protection
  - Accident and terrorism protection
- ...

measures

fencing	locks	access control cards	biometric access control systems
fire suppression systems	surveillance cameras	notification systems, such as intrusion detection sensors	heat sensors and smoke detectors.

Effectiveness of Controls

- Awareness of problem
  - People convined of the need for these controls
- Likelihood of use
  - Too complex/intrusive security tools are often disabled
- Overlapping controls
  - >1 control for a given vulnerability
    - To provide layered defense – the next layer compensates for a failure of the previous layer
- Periodic reviews
  - A given control usually becomess less effective with time
  - Need to replace ineffective/inefficient controls with better ones

Principles of Computer Security

- Principle of Easiest Penetration
  - An intruder must be expected to use any available means of penetration.
  - The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.

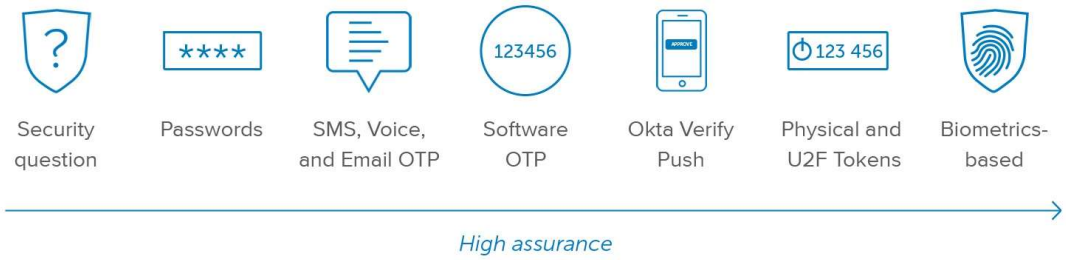
- Principle of Adequate Protection
  - Computer items must be protected to a degree consistent with their value and only until they lose their value.

[Pfleeger and Pfleeger]

- Principle of Effectiveness
  - Controls must be used—and used properly—to be effective.
  - They must be efficient, easy to use, and appropriate.

- Principle of Weakest Link
  - Security can be no stronger than its weakest link.
  - Whether it is the power supply that powers the firewall or the operating system under the security application or the human, who plans, implements, and administers controls, a failure of any control can lead to a security failure.

Authentication



- Persons accessing the information is who they say they are
- Factors of identification:
  - Something you know – user ID and password
    - User ID identifies you while the password authenticates you
    - Easy to compromise if weak password
  - Something you have – key or card
    - Can be lost or stolen
  - Something you are – physical characteristics (i.e., biometrics)
    - Much harder to compromise
- A combination of at least 2 factors is recommended

Access Control

- Once authenticated – only provide access to information necessary to perform their job duties to read, modify, add, and/or delete information by:
  - Access control list (ACL) created for each resource (information)
    - List of users that can read, write, delete or add information
    - Difficult to maintain all the lists
  - Role-based access control (RBAC)
    - Rather than individual lists
    - Users are assigned to roles
    - Roles define what they can access
    - Simplifies administration

Passwords

- Single-factor authentication (user ID/password) is the easiest to break
- Password policies ensure that this risk is minimized by requiring:
  - A certain **length** to make it harder to guess
  - Contain certain **characters** – such as upper and lower case, one number, and a special character
  - **Changing** passwords regularly and do not a password to be reused
  - Employees do **not share** their password
  - Notifying the security department if they feel their password has been **compromised**.
  - Yearly confirmation from employees that they understand their responsibilities

Backup

Important information should be backed up and store in a separate location

Very useful in the event that the primary computer systems become unavailable

A good backup plan requires:

- Understanding of the organizational information resources
- Regular backups of all data
- Offsite storage of backups
- Test of the data restoration

Complementary practices:

- UPS systems
- Backup processing sites

Cisco ASA

Fortigate

Palo Alto

Barracuda

Sophos

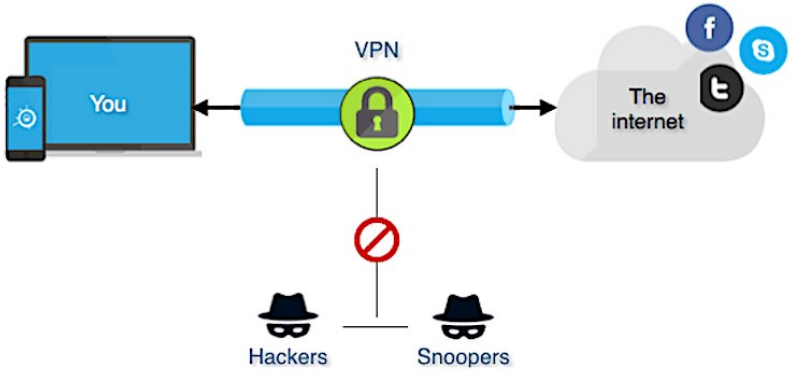
Check Point

Firewalls

- Can be a piece of hardware and/or software
- Inspects and stops packets of information that don't apply to a strict set of rules
  - Inbound and outbound
- Hardware firewalls are connected to the network
- Software firewalls run on the operating system and intercepts packets as they arrive to a computer
- Can implement multiple firewalls to allow segments of the network to be partially secured to conduct business
- Intrusion Detection Systems (IDS) watch for specific types of activities to alert security personnel of potential network attack

Virtual Private Networks (VPN)

- Some systems can be made private using an internal network to limit access to them
  - Can't be accessed remotely and are more secure
  - Requires specific connections such as being onsite
- VPN allows users to remotely access these systems over a public network like the Internet
  - Bypasses the firewall
  - Encrypts the communication or the data exchanged



Security Policies

- Starting point in developing an overall security plan
- Formal, brief, and high-level statement issued by senior management
  - Guidelines for employee use of the information resources
  - Embraces general beliefs, goals, objectives, and acceptable procedures
  - Includes company recourse if employees violate the policy
- Security policies focus on confidentiality, integrity, and availability
  - Includes applicable government or industry regulations
- Bring Your Own Device (BYOD) policies for mobile devices
  - Use when accessing/storing company information
  - Intellectual property implications
- Difficult to balance the need for security and users' needs

Personal Information Security

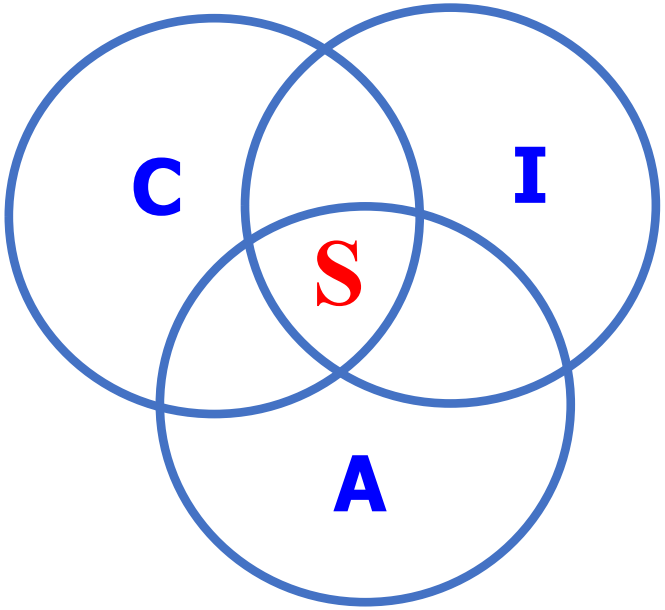
- Keep your software up to date
- Install antivirus software
- Use public networks carefully
- Backup your data
- Secure your accounts with two-factor authentication
- Make your passwords long, unique, and strong
- Be suspicious of strange links and attachments
- visit http://www.stopthinkconnect.org/

Information Security Principles
CIA vs CIAAAN

Dr. Bhaskar Mondal

CIA


INTEGRITY
AVAILABILITY
INFORMATION SECURITY
CONFIDENTIALITY


C
I
S
A

S = Secure

Security Mechanisms

Security Mechanisms

Cryptographic Techniques	Encryption and decryption methods
Software and hardware for access limitations	Firewalls
Intrusion Detection and Prevention Systems	Detect and prevent malicious packets
Traffic Padding	against traffic analysis
Hardware for authentication	Smartcards, security tokens
Security Policies / Access Control	define who has access to which resources.
Physical security	Keep it in a safe place with limited and authorized physical access

Cryptographic Security Mechanisms

Encryption (a.k.a. Encipherment)

use of mathematical algorithms to transform data into a form that is not readily intelligible (keys are involved)

Message Digest

similar to encryption, but one-way (recovery not possible)

generally no keys are used

Digital Signatures and Message Authentication

Data appended to, or a cryptographic transformation of, a data unit to prove the source and the integrity of the data

Authentication Exchange

ensure the identity of an entity by exchanging some information

Security Mechanisms

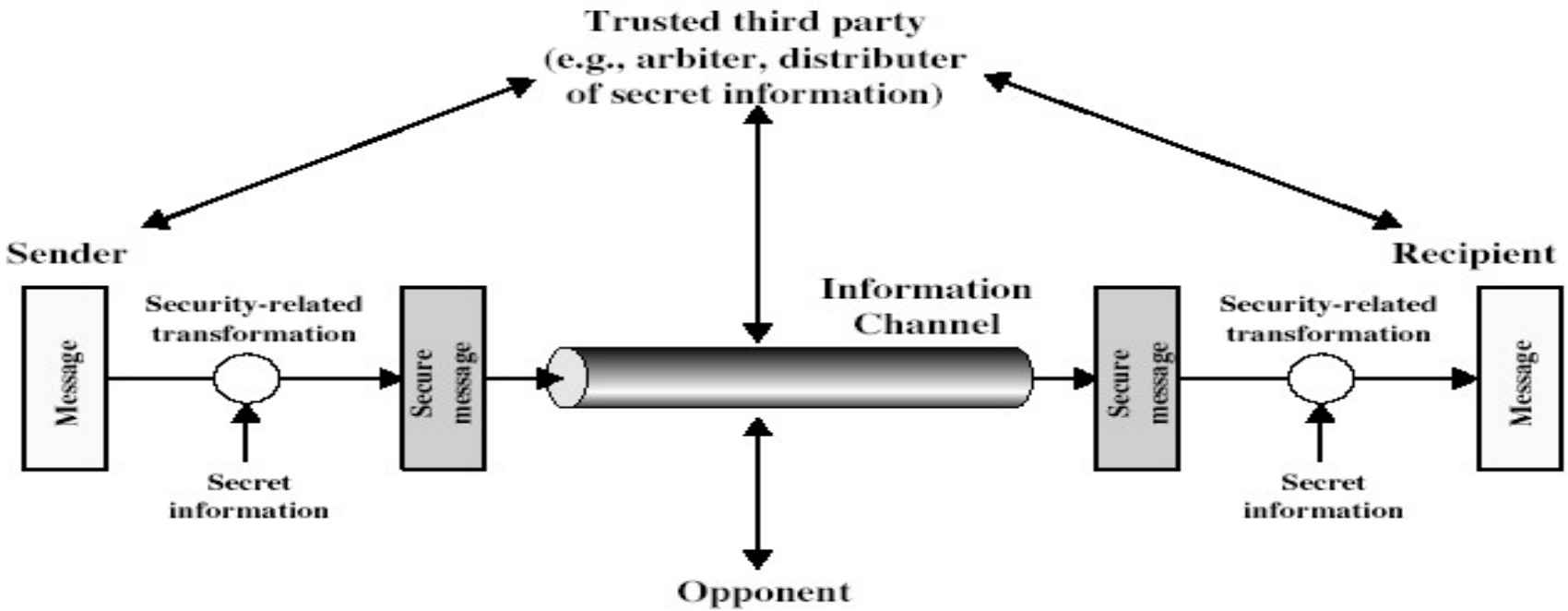
Notarization

use of a trusted third party to assure certain properties of a data exchange

Timestamping

inclusion of correct date and time within messages

A General Model for Network Security



Security Mechanisms (X.800)

Table 1.4 Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

http://www.itu.int/rec/T-REC-X.800-199103-I/e

Model for Information Security

01

design a suitable algorithm for the security transformation

02

generate the secret information (keys) used by the algorithm

03

develop methods to distribute and share the secret information

04

specify a protocol enabling the principals to use the transformation and secret information for a security service

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

About NIST and Standards

- "Founded in 1901 NIST, the National Institute of Standards and Technology, (former NBS) is a nonregulatory federal agency within the U.S. Commerce Department's Technology Administration.
- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life."
- Cryptographic Standards & Applications.
- Federal Information Processing Standards (FIPS): define security standards

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

- *Between security and ease-of-use*
- Security may require clumsy and inconvenient restrictions on users and processes

"If security is an add-on that people have to do something special to get, then most of the time they will not get it"

Martin Hellman,

co-inventor of Public Key Cryptography

Fundamental Tradeoff

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

"Everything should be as secure as necessary, but not securer"

Ravi Sandhu, "Good Enough Security", IEEE Internet Computing, January/ February 2003, pp. 66- 68.

- Read the full article at
  http://dx.doi.org/10.1109/MIC.2003.1167341

Good Enough Security

References

- William Stallings, Network Security Essentials : Applications and Standards, ISBN: 9788131761755, 8131761754

- Thanks to the many unknown sources from where some information is adopted.